IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re Dealer Management Systems Antitrust Litigation, MDL 2817

This document relates to:
Authenticom, Inc. v. CDK Global, LLC et al.,
Case No. 1:18-cv-00868 (N.D. Ill.)

No. 1:18-CV-864

Hon. Robert M. Dow, Jr.

Magistrate Judge Jeffrey T. Gilbert

COUNTERCLAIMANT THE REYNOLDS AND REYNOLDS COMPANY'S STATEMENT OF UNDISPUTED MATERIAL FACTS IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT

Counterclaimant The Reynolds and Reynolds Company ("Reynolds") files this Statement of Undisputed Material Facts in support of its Motion for Partial Summary Judgment, pursuant to Local Rule 56.1. As set forth in the accompanying Memorandum, this Motion seeks a partial summary judgment of liability as to certain of Reynolds' counterclaims against Authenticom.

STATEMENT OF UNDISPUTED FACTS

I. Reynolds owns and licenses the DMS to dealers pursuant to contracts that expressly limit system access to dealership employees

1. Reynolds owns, develops, and supports the Reynolds Dealer Management System ("DMS"). The Reynolds DMS is an enterprise computer software platform licensed by automotive dealerships to manage their business. Reynolds provides two DMS platforms, called ERA and POWER. ERA also has an enhanced user-interface version known as "ERA-IGNITE." Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 1, 6-7, 9, 14; Declaration of R. Lamb [Auth. Dkt. 98] ¶¶ 2, 4, 5-6; Ex. 1 at 34:3-16, 94:3-25 (Burnett tr.) (discussing ERA and ERA-Ignite); Ex. 2 at 63:22-64:2 (Kirby tr.).

2. The Reynolds DMS is comprised of multiple hardware and software components. The Reynolds DMS's "core" functionalities manage a dealer's accounting, parts, service, inventory, and sales operations. Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 2, 4; Declaration of R. Lamb [Auth. Dkt. 98] ¶¶ 2, 5.

3. Reynolds licenses its proprietary DMS to automotive dealerships pursuant to a license contract. That agreement expressly limits the scope of the Reynolds DMS license solely to dealership employees who have a need for access to operate the dealership's business. The agreement does not allow dealers to sublicense the Reynolds DMS, grant access to or share the DMS with any third parties, or connect any third-party software to the Reynolds DMS without Reynolds's express written permission. These restrictions are plain on the contracts' face, are well

known in the automotive industry, and have been in place for more than 12 years. Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 14, 17, 18; Declaration of R. Lamb [Auth. Dkt. 98] ¶ 3, 20-21; Ex. 3 at 314:3-11 (Brockman tr.); Ex. 4, REYMDL00677044 § 1 (Reynolds Master Agreement) ("You agree . . . not to disclose or provide access to any Licensed Matter or non-public portions of the Site to any third party, except your employees who have a need for access to operate your business and who agree to comply with your obligations under this Section[.]"); Ex. 5, REYMDL00012246 (Reynolds Customer Guide), at 256 ("You agree that you and third parties acting on your behalf have no right or authority to access or audit Reynolds' systems, applications, processes, procedures, or practices, except to the extent specifically authorized by Reynolds."), at 265 ("Unless we provide otherwise, you may not install Other Matter on the Equipment or connect Other Matter to Licensed Matter, either directly or remotely, without our prior written consent."), at 267 ("You expressly acknowledge that the Licensed Matter constitutes valuable proprietary property, includes confidential information and constitutes trade secrets that embody substantial create efforts and that is valuable to Reynolds. You agree to keep confidential the Licensed Matter (including all licensed copies and Documentation) covered under the Documents and shall not copy, reproduce, distribute, or in any way disseminate or allow access to or by third parties."); Ex. 6, REYMDL00675678 (Reynolds Defined Terms list); Ex. 92, REYMDL01075468 § 15.2.3 (Penske 2018 Agreement); Ex. 94, REYMDL00676893 (Reynolds Authorization Letter).

4. The Reynolds DMS license's restrictions on third-party access were also the subject of a 2012 lawsuit between Reynolds and a third-party data broker called Superior Integrated Solutions ("SIS"), which resulted in a federal court decision holding that Reynolds's DMS contracts forbid third-party access. Ex. 7, REYMDL00015586 ¶¶ 49-57 (Reynolds v. SIS Complaint); *Reynolds & Reynolds Co. v. Superior Integrated Sols., Inc.*, 1:12-CV-848, 2013 WL

2456093, at *2 (S.D. Ohio June 6, 2013). SIS subsequently agreed to a settlement whereby it would wind down its hostile access to the Reynolds DMS. Ex. 8, REYMDL00022780 (Reynolds-SIS Settlement Agreement).

5. When a user accesses the Reynolds ERA DMS, they do so via a program called ERAccess.exe or ERA-Ignite.exe. Both programs are Reynolds's registered copyrighted intellectual property. Ex. 9 (Copyright TX 7-586-896); Ex. 10 (Copyright TX 7-586-863); Ex. 11 (Copyright TX 8-538-825); Ex. 12 (Copyright TX 8-538-541). A user must first enter a valid set of credentials (user ID and password). After entering those credentials, they are then able to access the rest of the ERA system, which is also Reynolds's copyrighted (although not registered) intellectual property. *See* Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 14 (Testimony of R. Schaefer); Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 4, 14, 27; Ex. 13 (Login screen for ERAccess, version 27.250); Ex. 14, REYMDL00022920 (Aug. 19, 2010 ERAccess announcement); Ex. 15, REYMDL00022918 (Jan. 14, 2011 ERAccess announcement).

II. Dealers' operational data is available without unauthorized access to the DMS

6. Reynolds has developed software tools that allow dealership employees to export dealers' operational data from the Reynolds DMS. The current version of this tool is called Dynamic Reporting. Dynamic Reporting allows dealer employees to create custom reports with their specified data fields and formats. Reports can be saved, and any report can be scheduled to run automatically up to four times a day. Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 86; Ex. 23 at 42:19-44:6 (Reynolds 30(b)(6) Hall tr.).

7. Once a dealership employee has exported a dealership's operational data from the Reynolds DMS, Reynolds places no contractual or technological restrictions on the dealership's use of that data. Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 87.

8. Some dealers choose to send or transmit data that they exported from the Reynolds DMS using Dynamic Reporting to Authenticom. Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 87; Ex. 24 at 70:10-19 (Wiersgalla tr.); Ex. 44 at 141:12-142:21 (Hembd tr.); Ex. 96, AUTH_00150633.

9. In addition, Reynolds offers its dealership customers the option of having Reynolds automatically transfer the dealerships' vehicle inventory data (data that does not contain any sensitive personally identifiable information) to an FTP site through Reynolds's AVID (Automated Vehicle Inventory Data) product. Once the data is moved outside of the DMS, Reynolds places no contractual or technical restrictions on the dealership's ability to provide access to this data, including to Authenticom. Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 90; Ex. 39 at 188:8-189:14 (Munns tr.); Ex. 95, AUTH_00067483.

III. Reynolds undertakes a persistent, widely publicized campaign to eradicate unauthorized third-party access to its proprietary DMS

10. Reynolds merged with another DMS provider, Dealer Computer Services, in 2006. Dealer Computer Systems owned the POWER DMS product, while Reynolds owned the ERA DMS product. At that time, POWER was a secure, stable DMS platform that enjoyed the benefit of that reputation in the marketplace. ERA, in contrast, had serious security holes. For example, the ERA DMS was still using dial-up modems for communications. After the merger, Reynolds worked to improve ERA's security. Ex. 3 at 15:1-16:23; 303:9-304:11 (Brockman tr.); Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 7, 9, 28-30; Ex. 16 at 31:24-33:9 (Lamb tr.).

11. A core part of Reynolds's security strategy was to eliminate the security holes that were being exploited by third parties to hostilely access to the Reynolds DMS. Mr. Brockman and others at Reynolds regularly announced this policy and strategy to the automotive industry and industry publications widely reported it. Ex. 3 at 304:12-25 (Brockman tr.); Ex. 17 (January 2007

Automotive News Article); Ex. 107, REYMDL00012341 (February 2007 Automotive News Article) ("Reynolds, with about 11,000 dealership customers in the United States, has warned dealers that they are violating their contracts when they provide log-ins and passwords to third-party vendors."); Ex. 18, REYMDL00022899 (Fuel Article January 1, 2010: "It remains our policy to not allow 'hostile interfaces' or unauthorized code on your systems to protect both Reynolds and your dealership from security breaches and potential data corruption issues."); Ex. 108 (same Fuel article, submitted by Authenticom as preliminary injunction exhibit 14 [Auth. Dkt. 64-14]; Ex. 19 (AUTH_00170940) (Authenticom 2013 announcement that [redacted]").

12. Reynolds took early steps to better secure and control access to its ERA DMS. These steps included:

- Requiring all dealership employees to use a unique set of login credentials (including a user ID and password) to access the DMS;
- Removing all third-party software from Reynolds DMS servers;
- Ending modem access to the Reynolds DMS;
- Requiring regular DMS password changes; and
- Requiring Reynolds DMS users to use only Reynolds's approved terminal software to access the DMS.

Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 29-30; Ex. 20, REYMDL00015519 (2016 ERA Data Management Milestones); Ex. 21, REYMDL00015521 (2011 ERA Data Management Milestones).

13. Reynolds continued to implement access control measures over time. For example, Reynolds implemented CAPTCHA prompts and challenge questions, which require users to answer questions intended to prove they are human dealership employees. CAPTCHA prompts are a form of Turing test; their purpose is to prevent automated processes or machines from

assessing a computer system. Ex. 16 at 64:23-65:6 (Lamb tr.); Ex. 22 at 68:4-9 (Hill tr.); Ex. 23 at 48:7-18 (Reynolds 30(b)(6), Hall tr.); Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 30; Ex. 24 at 86:4-24 (Wiersgalla tr.); Ex. 25 at 337:23-338:22 (SIS 30(b)(6), Battista tr.).

14. Reynolds first introduced its “Challenge Questions” (e.g., “What color is the sky?”) in 2009. Reynolds then introduced ASCII CAPTCHAs in 2010, and later replaced those with graphical CAPTCHAs starting in 2012. Ex. 20, REYMDL00015519 (2016 ERA Data Management Milestones); Ex. 26, AUTH_00468320 (Authenticom timeline chart [redacted]); Ex. 27, REYMDL00101073 at 23 (showing CAPTCHA security check prompt); Ex. 28 at 46:14-17, 48:13-24 (Clements tr.) [redacted]); Ex. 16 at 65:7-17 (Lamb tr.) (describing Reynolds’s long history of CAPTCHA use); Declaration of S. Cottrell [Auth. Dkt. 51] ¶ 37 [redacted]”); Ex. 29 at 172:7-11 (Cottrell 2019 tr.) (“[redacted].”); Authenticom Resp. to Defs. Statement of Add’l Facts [Auth. Dkt. 145] (hereinafter “Auth. Resp. to DSAF”) ¶¶ 75, 76 (“Undisputed that Reynolds implemented a series of roadblocks to prevent dealers from using independent integrators, including challenge questions and captcha.”).

15. Reynolds also developed a “Suspicious User ID” detection system, which detected [redacted]. Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 15, 16 (Testimony of R. Schaefer); Ex. 30, REYMDL00001971, at 1976-1977 (ERA May 2013 Release Notes).

16. On August 8, 2011, Reynolds announced the rollout of this security enhancement that monitored, detected, and disabled user IDs using automated access methods. Ex. 31, REYMDL00022904 (August 8, 2011 Reynolds System Announcement); Declaration of S. Cottrell [Auth. Dkt. 51] ¶ 37.

17. In May 2013, Reynolds released the enhanced version of this monitoring system, known as the Suspicious User ID process, for its ERA DMS. As described in the user guide for this release, the process was used to track and prevent suspicious system activity. Any user ID attempting to access the system with software or a communications method not supported by Reynolds—i.e., any hostile or automated method—would be immediately disabled. *See* Ex. 30, REYMDL00001971, at 1976-1977; Auth. Resp. to DSAF [Auth. Dkt. 145] ¶ 77; Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 30; Ex. 32, AUTH_00219452 (containing examples of disabled Authenticom IDs and associated screenshots from the Reynolds DMS); Declaration of S. Cottrell [Auth. Dkt. 51] ¶ 38 (testifying that Reynolds disabled 27,000 profiles used by Authenticom in summer 2013).

18. Reynolds's monitoring process [redacted]). As part of its Suspicious User ID measure, the Reynolds system [redacted]. If a user ID fails the Reynolds criteria, the ID is deemed suspicious and its access to the Reynolds DMS is disabled. Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 15, 16 (Testimony of R. Schaefer); Ex. 33, AUTH_00141204; Ex. 34,

AUTH_00093108; Ex. 35, AUTH_00141219; Ex. 36, AUTH_00167914; Ex. 32, AUTH_00219452.

19. These access-control measures were targeted at a variety of potential threats, including (a) any attempts to access the Reynolds DMS through automated scripts or programs and (b) any attempts by non-dealer-employees to access the Reynolds DMS. Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 15, 16 (Testimony of R. Schaefer); Auth. Resp. to DSAF [Auth. Dkt. 145] ¶ 77; Declaration of S. Cottrell [Auth. Dkt. 51] ¶¶ 37-38; Ex. 20, REYMDL00015519 (2016 ERA Data Management Milestones).

20. One group that sought to access the Reynolds DMS through automated methods were the so-called "third-party integrators," or as Reynolds called them, "hostile integrators," "hackers," and "bandits." Ex. 3 at 314:12-315:4 (Brockman tr.); Ex. 37 at 28:12-18 (Hellyer tr.); Ex. 38 at 33:21-34:8 (Martin tr.); Ex. 16 at 217:5-15 (Lamb tr.); Ex. 23 at 19:18-20:25 (Reynolds 30(b)(6) Hall tr.).

IV. Authenticom's automated access methods to the Reynolds DMS

21. Authenticom was a third-party data broker throughout the relevant time period. Authenticom's business model with respect to the Reynolds DMS was predicated on using automated scripts to access the Reynolds DMS, utilize the DMS's internal features and functionality to display and report data, and exfiltrate that data back to Authenticom's servers. Authenticom referred to this process as "polling" a DMS. Authenticom would subsequently send that data on to third parties such as application vendors. *See generally* Ex. 33, AUTH_00141204 (Overview of R&R Polling); Declaration of S. Cottrell [Auth. Dkt. 51] ¶¶ 9, 25.

22. Authenticom also had available to it, and sometimes used, other methods to obtain data from the Reynolds DMS. Authenticom's primary alternative method involved having dealers export data themselves from the DMS (for example, using Reynolds's Dynamic Reporting

application) and then transmit the exported data to Authenticom. [redacted] Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 87; Ex. 24 at 70:10-19, 93:7-94:17 (Wiersgalla tr.); Ex. 44 at 141:12-142:21 (Hembd tr.); Ex. 96, AUTH_00150633.

A. Authenticom obtains user IDs intended solely for dealership employees

23. [redacted]. Ex. 28 at 118:16-22 (Clements tr.); Ex. 33, AUTH_00141204 (Overview of R&R Polling); Ex. 39 at 43:2-46:7 (Munns tr.).

24. To accomplish this, Authenticom would reach out to the dealer that had licensed the Reynolds DMS in question and ask them to provide one or more sets of DMS user credentials. [redacted] Ex. 28 at 151:10-152:13 (Clements tr.); Ex. 39 at 25:17-26:7, 247:14-248:15 (Munns tr.); Ex. 40 at 49:14-50:6 (Auth. 30(b)(6) Brown tr.); Ex. 41, AUTH_00431252; Ex. 42, AUTH_00431361; Ex. 43, AUTH_00170533; Auth. P.I. Tr. 1-A [Auth. Dkt. 164] at 108:4-19 (Testimony of S. Cottrell).

25. [redacted]

[redacted] Ex. 39 at 43:19-44:7, 52:1-55:6 (Munns tr.); Ex. 33, AUTH_00141204 (Overview of R&R Polling); Ex. 2 at 62:7-63:7, 290:8-291:23 (Kirby tr.).

B. Authenticom's polling process relied on launching Reynolds software on Authenticom's servers

26. [redacted] Ex. 39 at 113:17-115:18 (Munns tr.); Ex. 2 at 161:11-162:23 (Kirby tr.); Ex. 28 at 146:14-147:15 [redacted]); Ex. 33, AUTH_00141204 (Overview of R&R Polling).

27. [redacted] Ex. 39 at 38:15-39:2 (Munns tr.); Ex. 2 at 161:11-166:25 (Kirby tr.); Ex. 44 at 120:22-121:16 (Hembd tr.); Ex. 28 at 99:22-103:16 (Clements tr.); Ex. 40 at 200:11-203:8 (Auth. 30(b)(6) Brown tr.).

28. [redacted] Ex. 33, AUTH_00141204 (Overview

of R&R Polling); Ex. 2 at 47:24-49:19 (Kirby tr.); Ex. 40 at 137:8-140:9, 142:10-143:1 (Auth. 30(b)(6) Brown tr.).

C. Authenticom works to circumvent Reynolds's access controls

29. As Reynolds introduced various controls to prevent automated third parties from accessing it DMS, Authenticom worked to circumvent or create workarounds for each of those measures in turn. Auth. P.I. Tr. 1-P [Auth. Dkt. 162] at 44:10-14 (Testimony of S. Cottrell) (admitting that from 2010 to 2017, Reynolds had been "actively blocking" Authenticom and Authenticom "does what it can to get around those blocks"); Authenticom Mot. for P.I. at 8 [Auth. Dkt. 61] (stating that Authenticom worked to "develop workaround solutions that circumvented Reynolds's efforts to block access"); Auth. 7th Cir. Resp. Br. at 12 ("Reynolds' efforts, however, were not entirely successful; Authenticom, CDK, and other integrators worked with dealers to develop workarounds."); Ex. 26, AUTH_468320 ([redacted]).

1. Authenticom's efforts to circumvent Reynolds's CAPTCHA prompts

30. As set forth above, Reynolds implemented CAPTCHA prompts and challenge questions to prevent automated processes from accessing its DMS beginning in 2009. Authenticom developed various ways for its automated polling programs to get around Reynolds's CAPTCHA prompts. Ex. 45 at 75:6-80:11 (Robinson tr.); Ex. 28 at 31:16-32:17 (Clements tr.); Ex. 26, AUTH_468320.

31. First, [redacted] Ex. 39 at 140:4-5, 148:11-149:19

(Munns tr.); Ex. 29 at 268:12-22 (Cottrell 2019 tr.); Ex. 45 at 77:5-10, 80:9-11 (Robinson tr.); Ex. 46, AUTH_00096097; Ex. 47, AUTH_00091915.

32. [redacted] Ex. 48, AUTH_00095693; Ex. 39 at 152:3-7 (Munns tr.). [redacted] Ex. 49, AUTH_00083390.

33. Authenticom also utilized CAPTCHA farms to answer Reynolds's CAPTCHA prompts. [redacted] Ex. 33, AUTH_00141204; Ex. 28 at 138:5-16 (Clements tr.).

34. [redacted] Ex. 50, AUTH_00280874; Ex. 51, AUTH_00280909; Ex. 52, AUTH_00280913; Ex. 53, AUTH_00280915; Ex. 54, AUTH_00280937; Ex. 55, AUTH_00281398; Ex. 56, AUTH_00281333; Ex. 57, AUTH_00281303; Ex. 58, AUTH_00281301; Ex. 59, AUTH_00281253; Ex. 60, AUTH_00315748; Ex. 61, AUTH_00281205; Ex. 62, AUTH_00281015; Ex. 63, AUTH_00280991; Ex. 64, AUTH_00280958; Ex. 82, AUTH_00281367; Ex. 65 at 79:19-88:9 (Noth tr.).

35. Authenticom also used [redacted] Ex. 40 at 172:3-22 (Auth. 30(b)(6) Brown tr.).

36. Authenticom also [redacted] Ex. 40 at 170:15-171:16, 172:3-22 (Auth. 30(b)(6) Brown tr.); Ex. 66, AUTH_00092449 (discussing [redacted]).

37. Authenticom also used [redacted] Ex. 40 at 161:4-8 (Authenticom 30(b)(6) Brown tr.); Ex. 46, AUTH_00096097; Ex. 67, AUTH_00092111 ([redacted]).

2. **Authenticom's efforts to avoid Reynolds's Suspicious User ID measure**

38. Authenticom engaged in a long-running campaign to avoid having its IDs detected and disabled by Reynolds's security measures. Ex. 68, AUTH_00171450 [redacted]); Ex. 33, AUTH_00141204 ([redacted]); Ex. 26, AUTH_00468320.

39. Authenticom asked Reynolds dealers [redacted] As stated by [redacted].” Ex. 69, AUTH_00168020. Authenticom's goal was to avoid detection by Reynolds. Ex. 70, AUTH_00168116 (“[redacted]”).

40. [redacted] Ex. 39 at 105:13-21 (Munns tr.); Ex. 32, AUTH00219452.

41. [redacted] Ex. 39 at 107:8-12 (Munns tr.). As described by Authenticom, [redacted]

[redacted]” Ex. 71, AUTH_00465304. In other words, [redacted] Ex. 72, AUTH_00230422, at 5 ([redacted]); Ex. 73, AUTH_00242735 (“[redacted]); Ex. 26, AUTH_00468320 ([redacted]).

42. [redacted] Ex. 34, AUTH_00093108.

43. [redacted] Ex. 74, AUTH_00168432. [redacted] Ex. 75, AUTH_00101801. [redacted] Ex. 76, AUTH_00154490 at 493.

44. [redacted] Ex. 77, AUTH_00221025; Ex. 78, AUTH_00091792.

45. Authenticom also [redacted] As stated by Authenticom employees, [redacted]

[redacted] Ex. 36, AUTH_00167914.

46. Authenticom eventually [redacted] Ex. 33, AUTH_00141204.

47. Authenticom [redacted]. Ex. 36, AUTH_00167914; Ex. 79, AUTH_00170407; Ex. 35, AUTH_00141219; Ex. 68, AUTH_00171450.

48. [redacted] Ex. 39 at 113:17-115:18 (Munns tr.); Ex. 80, AUTH_00094637 (email chain re "[redacted]"); AUTH_00174085 ("[redacted]"). [redacted]" Ex. 33, AUTH00141204.

V. Authenticom's conduct was knowing, intentional, and without authorization from Reynolds.

49. Authenticom knew that its access to the Reynolds DMS was unauthorized by Reynolds. Reynolds had informed the world since at least 2007 that it did not approve of third parties accessing its DMS. Reynolds made repeated announcements to its customer base and the market that third-party access to its DMS was prohibited. Ex. 82 (February 19, 2007 Automotive News Article); Ex. 107, REYMDL00012341 (February 4, 2007 Automotive News Article) ("Reynolds, with about 11,000 dealership customers in the United States, has warned dealers that

they are violating their contracts when they provide log-ins and passwords to third-party vendors."); Ex. 97, REYMDL00015601 (April 2007 Automotive News Article) (reporting that in 2006 "Reynolds and Reynolds Co. began informing dealers they would be violating their contract if they allowed third parties to access directly the Reynolds dealer management system"); Ex. 98, REYMDL01075600 (March 2012 Automotive News Article) ("What we're [Reynolds] trying to do is block unmonitored automated access to the DMS."); Ex. 18, REYMDL00022899 (Fuel Article January 1, 2010: "It remains our policy to not allow 'hostile interfaces' or unauthorized code on your systems to protect both Reynolds and your dealership from security breaches and potential data corruption issues."); Authenticom Compl. [Auth. Dkt. 1] ¶¶ 6, 92, 103, 106-107, 109, 185.

50. Reynolds backed those announcements with concrete enforcement steps, and Authenticom was aware of Reynolds's policy and desire to prevent third parties from accessing its DMS without Reynolds's permission. Ex. 93, REYMDL00015727 (Authenticom receiving Reynolds's 2011 announcement that it was rolling out measures to prevent automated access to the Reynolds system); Ex. 26, AUTH_00468320 ([redacted]); Ex. 83, AUTH_00472681 ([redacted]); Ex. 84, AUTH_00170766 [redacted]).

51. Authenticom announced to its customer base in 2013 that Reynolds was "[redacted]." Ex. 19, AUTH_00170940.

52. Authenticom's executives admitted [redacted]. Ex. 29 at 21:11-12 (Cottrell 2019 tr.) ("[redacted]"); Ex. 85 at 100:1-6; 128:14-16 (Gentry tr.) [redacted]); Ex. 28 at 60:5-63:22 (Clements tr.) ([redacted]); Ex. 86, AUTH_00091619, at 621.

53. [redacted] Ex. 29 at 270:10-19 (Cottrell 2019 tr.).

54. The ERA DMS login screen—seen every time a user accesses the system—further announced Reynolds's prohibition on any copying, accessing, or use of the system by any third party. Authenticom employees [redacted] Ex. 87, AUTH_00175368; Ex. 88, AUTH_00472396; Ex. 89, AUTH_00155147, at 151; Ex. 39 at 351:13-356:19 (Munns tr.); Ex. 2 at 174:22-179:4 (Kirby tr.); Ex. 44 at 121:18-128:20 (Hembd tr.).

55. Reynolds also sent Authenticom an express cease-and-desist letter in 2015, demanding that it cease accessing the Reynolds DMS. Ex. 91, REYMDL00012553.

56. Reynolds provided the court's ruling in the *SIS* case to Authenticom, along with the contractual language it was based upon. Ex. 90, AUTH_00468019.

[Signature block on following page]

Dated: October 15, 2019

Respectfully submitted,

/s/ *Aundrea K. Gulley*
Aundrea K. Gulley
Brian T. Ross
Brice A. Wilkinson
Ross A. MacDonald
GIBBS & BRUNS LLP
1100 Louisiana Street
Suite 5300
Houston, TX 77002
(713) 751-5258
agulley@gibbsbruns.com
bross@gibbsbruns.com
bwilkinson@gibbsbruns.com
rmacdonald@gibbsbruns.com

Michael P.A. Cohen
Leo D. Caseria
SHEPPARD MULLIN RICHTER & HAMPTON, LLP
2099 Pennsylvania Avenue NW, Suite 100
Washington, DC 20006
(202) 747-1900
mcohen@sheppardmullin.com
lcaseria@sheppardmullin.com

Counsel for Defendant
The Reynolds and Reynolds Company

CERTIFICATE OF SERVICE

I, Brice A. Wilkinson, an attorney, hereby certify that on October 15, 2019, I caused a true and correct copy of the foregoing **COUNTERCLAIMANT THE REYNOLDS AND REYNOLDS COMPANY'S STATEMENT OF UNDISPUTED MATERIAL FACTS IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT** to be filed and served electronically via the court's CM/ECF system. Notice of this filing will be sent to all parties at the following email address: SERVICE-EXTERNAL-DMS-MDL@lists.kellogghansen.com.

/s/ Brice A. Wilkinson
Brice A. Wilkinson
Gibbs & Bruns LLP
1100 Louisiana Street
Suite 5300
Houston, TX 77002
(713) 751-5218
bwilkinson@gibbsbruns.com